Actualités informatiques pour
la magistrature

AIM

OUTIL ESSENTIEL : LE GUIDE CANADIEN POUR LA PRÉPARATION UNIFORME DES JUGEMENTS

Au fur et à mesure que la publication électronique des jugements deviendra la norme, la normalisation de leur format assurera un maximum d'avantages aux tribunaux, aux avocats, aux éditeurs et au public.

Le Comité consultatif sur l'utilisation des nouvelles technologies par les juges, avec l'aide du Comité canadien de la référence (CCR), a fait œuvre de pionnier en généralisant les meilleures pratiques en matière de préparation des jugements et de simplification de la publication de la jurisprudence.

Une autre étape très importante a été franchie grâce à la publication du *Guide canadien pour la préparation uniforme des jugements*, lequel :

- révise les *Normes relatives à la façon de rédiger, de distribuer et de citer les jugements canadiens sous forme électronique* adoptées en 1996;
- prend appui sur la *Norme de référence neutre pour la jurisprudence* adoptée en 1999.

Toutes les cours et tous les tribunaux sont invités à mettre en œuvre les normes ci-haut. L'accent porte sur la normalisation des éléments les plus essentiels, sans que ne soit alourdie la tâche du personnel affecté à la préparation des jugements. Le Guide s'applique à toutes les décisions judiciaires rendues par les cours supérieures au Canada et par toute autre cour ou tout autre tribunal qui adopte les normes. Il énonce les meilleures pratiques relatives au format électronique des jugements distribués sous forme de fichier.

Le Guide reflète une compréhension accrue du document électronique et des conditions requises pour en tirer tous les bénéfices. Il améliore et complète les normes existantes, en mettant l'accent sur la normalisation des éléments essentiels à l'identification des jugements dans une base de données consultable, tels que la référence, la date et le numéro de dossier. On laisse à chaque tribunal le soin de décider de l'apparence de ses jugements.

En vertu du mode de dénomination des fichiers prévu par le Guide, chaque fichier se voit accorder un nom unique et significatif qui en facilite la gestion et la distribution. Le Guide énonce également les normes relatives au traitement de fichiers non textuels, tels que les images, et de divers types de documents émis par les tribunaux, tels que les motifs multiples, les versions en différentes langues, les motifs supplémentaires et les corrections apportées à un jugement.

En tant que conseiller technique auprès du Comité consultatif sur l'utilisation des nouvelles technologies par les juges, le professeur Daniel Poulin, du Centre de recherche en droit public de l'Université de Montréal, est le coordonnateur du CCR. Vous pouvez communiquer avec lui par téléphone au (514) 343-2139 ou par courriel à poulind@droit.umontreal.ca. Les

Voir ...

tribunaux peuvent obtenir une assistance directe relativement à la mise en œuvre du Guide en visitant le site Web du CCR (www.lexum.umontreal.ca/ccc-ccr/index_en.html) ou en communiquant avec Frédéric Pelletier, secrétaire du CCR, par courriel (pelletif@lexum.umontreal.ca) ou par téléphone (514-343-6111, 1-3257).

Le Guide est disponible à l'adresse suivante : www.cjc-ccm.gc.ca/francais/publications/Guide.fr.pdf.

RISQUE CACHÉ : LE PROBLÈME DES MÉTADONNÉES DANS LES DOCUMENTS

Les documents préparés au moyen d'un logiciel de traitement de texte courant tel que Word ou Word Perfect contiennent divers types de renseignements plus ou moins dissimulés que l'on appelle métadonnées.

Les métadonnées sont des éléments de texte ajoutés par un logiciel au texte principal d'un document. Elles peuvent être aussi anodines que des directives de formatage. Toutefois, elles peuvent aussi renseigner sur l'historique du document, y compris le texte des versions antérieures, les fragments de texte supprimés ou ajoutés, ainsi que les commentaires des réviseurs.

Puisque les métadonnées peuvent être lues par le récipiendaire d'un document, il existe un risque grave que des renseignements sensibles soient divulgués lors de la distribution de documents.

Heureusement, il est possible de prendre certaines précautions.

Les métadonnées peuvent être minimisées en utilisant les fonctions du logiciel de traitement de texte ayant servi à créer le document ou des logiciels spécialisés qui nettoient les documents. Certains types de métadonnées ne sont accessibles que grâce à un « éditeur de texte générique » qui peut, par exemple, donner accès aux dix derniers auteurs d'un document Word.

Le professeur Daniel Poulin et l'assistant à la recherche Frédéric Pelletier, du Centre de recherche en droit public de l'Université de Montréal, ont rédigé un document intitulé *La préparation des documents pour distribution électronique*, lequel propose des procédures visant le traitement des questions relatives aux métadonnées. Le document recommande des procédures visant la préparation des documents pour distribution électronique afin de réduire les risques liés aux renseignements confidentiels et décrit les outils logiciels permettant de minimiser automatiquement les métadonnées dans les documents.

Le document est disponible à l'adresse suivante : www.lexum.umontreal.ca/citation/guide/en/distribution.fr.html.

CONSEILS EN MATIÈRE DE SÉCURITÉ : (SURTOUT) À L'INTENTION DES UTILISATEURS DE JUDICOM

Dans le numéro 32 des *Actualités informatiques pour la magistrature* (printemps 2002), le Sous-comité sur la sécurité informatique du Comité consultatif sur l'utilisation des nouvelles technologies par les juges a présenté aux juges dix conseils sur l'amélioration de la sécurité des données judiciaires. Ceux-ci sont disponibles sur le site Web du Conseil canadien de la magistrature, à l'adresse suivante : www.cjc-ccm.gc.ca.

Des conseils similaires s'appliquant tout particulièrement aux utilisateurs de Judicom sont maintenant disponibles en plus de détails dans un document intitulé *35 conseils en matière de sécurité informatique*, qui a été préparé par le Partenariat de formation informatisée dans le cadre d'un projet conjoint du Bureau du Commissaire à la magistrature fédérale et de l'Institut national de la magistrature.

Les conseils propres à Judicom traitent notamment de l'utilisation d'Internet et du courrier électronique de Judicom. Les conseils abordent également de façon plus approfondie la protection par mot de passe et la protection antivirus.

Les conseils sont disponibles à l'adresse suivante : www.cep.njicourses.ca/comptrng/contents/security_tips.html.

TÉLÉPHONES SANS FIL ET TÉLÉPHONES CELLULAIRES : PRÉSUMEZ QU'ON VOUS ENTEND

Lorsque le juge Robert Carr a traversé le Canada en tant que membre de l'équipe de formation de Judicom, il a été surpris d'apprendre que les juges s'intéressaient avant tout à l'utilisation sécuritaire de leurs téléphones! Voici ce qu'il leur a dit.

Les téléphones sans fil constituent dans la plupart des foyers une solution pratique aux modèles conventionnels. Les téléphones cellulaires sont tout aussi populaires. Les juges suivent eux aussi les tendances en matière de téléphone sans fil et de téléphone cellulaire.

Toutefois, plusieurs juges ne savent pas que l'utilisation même prudente de tels appareils les expose à un risque grave de violation de la vie privée et à l'interception de renseignements confidentiels.

Téléphones sans fil

Les téléphones sans fil et autres appareils émetteurs de signaux, tels que les moniteurs sans fil pour bébés, sont des mini-radios dont les signaux peuvent être captés par certains appareils, y compris d'autres téléphones et antennes tournantes. Selon les conditions et l'équipement, la portée radio peut varier d'environ un demi-kilomètre à trois kilomètres. Les antennes tournantes sont aisément disponibles sur Internet et dans certains magasins de détail. Elles sont tout à fait légales, peu coûteuses et très populaires.

Téléphones cellulaires

Les téléphones cellulaires envoient des signaux radio à des émetteurs de faible puissance, des « cellules » ayant habituellement un rayon de 8 à 19 kilomètres. Par exemple, dans une automobile, alors que l'utilisateur se déplace d'une cellule à une autre, le signal est transmis à l'émetteur le plus proche et peut dans certains cas être capté par une antenne tournante.

De plus, un téléphone cellulaire peut être « cloné » grâce à un lecteur « NSE »; l'appareil lit simplement le numéro de série électronique du téléphone et le reprogramme sur une puce d'ordinateur dans un autre téléphone cellulaire, de manière à permettre au voleur d'utiliser la ligne téléphonique de sa victime.

Minimiser les risques

Mes conseils :

- Premièrement, ne discutez évidemment de questions confidentielles qu'à partir d'une ligne terrestre, laquelle est essentiellement sécuritaire.
- Débarrassez-vous de votre téléphone analogique (sans fil ou cellulaire). Le téléphone analogique génère un signal constant, ininterrompu et facilement captable. De plus, ne le traitez pas comme un vieux matelas, par exemple en continuant à l'utiliser au chalet. Remplacez vos téléphones analogiques par des modèles numériques. Les téléphones numériques coupent constamment le signal et le numérisent pour résister à la surveillance. Achetez un téléphone de qualité. Quant à la qualité et la distance, assurez-vous d'obtenir une fréquence d'au moins 2,4 mégahertz et insistez sur la technologie ENS (étalement numérique du spectre), qui permet de sauter d'une fréquence à l'autre et rend presque impossible l'interception du signal.
- Achetez votre téléphone chez un détaillant bien informé et interrogez-le sur la question de la sécurité. Si vous choisissez un spécialiste de l'électronique fiable, vous serez moins vulnérable.

Le juge Robert Carr est juge de la Cour du Banc de la Reine du Manitoba et président du comité directeur de Judicom.

PERSPECTIVES SUR LE PROJET D'INTÉGRATION DU SYSTÈME JUDICIAIRE DE L'ONTARIO

« Certains aspects importants du Projet d'intégration du système judiciaire de l'Ontario n'ont pas connu de succès [...] en pratique, le Projet tire à sa fin ».
– le juge N. D. Coo

« [...] on peut tirer des leçons de l'échec de cette initiative. »
– le juge B. T. Granger

Les juges N. D. Coo et B. T. Granger de la Cour supérieure de justice de l'Ontario ont donné leurs perspectives franches sur la tentative ambitieuse visant à créer un environnement électronique commun sur l'ensemble du système judiciaire de l'Ontario.

Lors de récents discours, les deux juges ont précisé que leurs collègues devaient être à l'avant-plan des décisions concernant la technologie informatique qui sera à la disposition de leurs tribunaux à l'avenir.

Lors d'une présentation devant une réunion d'experts de la conférence internationale Internet pour le droit à Montréal, le juge Coo a déclaré que le Projet d'intégration du système judiciaire de l'Ontario avait « connu de graves difficultés financières, politiques et techniques, de sorte qu'il ne survivra pas dans sa forme actuelle ». Les juges étaient des conseillers plutôt que des associés dans le cadre du projet et l'expérience a démontré que « la magistrature ne devrait pas permettre l'élaboration d'un tel projet sans qu'elle n'y participe elle-même de façon plus active et responsable ».

Il a déclaré que le projet avait pour but la création d'une base de données électronique commune et partagée à l'intention des tribunaux, des juges, des avocats de façon générale, des procureurs de la Couronne, de la police, du système de garde et du système correctionnel, afin que les renseignements ne doivent être notés, créés, enregistrés, mis en mémoire et archivés électroniquement qu'une seule fois en matière criminelle, civile ou familiale.

L'intégration d'un programme de gestion des instances fondé sur Internet s'est heurtée à des problèmes importants, de sorte que les tribunaux se sont retrouvés sans un accès complet à la base de données, aux programmes de gestion d'agenda et d'établissement de calendrier ou aux statistiques de gestion.

Le juge Coo a précisé qu'une certaine forme de système intégré ferait son apparition et que les juges ne devaient pas permettre aux tiers « d'usurper ce qui devrait être le rôle judiciaire des chefs de tribunaux ni d'assumer la responsabilité exclusive de l'administration des tribunaux. En plus d'en être responsables, les juges doivent participer pleinement à tout nouveau système qui affectera fondamentalement presque toutes les facettes des travaux du tribunal ».

Lors d'un discours prononcé devant l'Association canadienne des juges des cours supérieures, dans le cadre de l'assemblée annuelle de l'Association du Barreau canadien à London, le juge Granger a déclaré que les problèmes du système étaient particulièrement graves à la Cour de la famille de la Cour supérieure de justice, qui a adopté des règles relatives à la gestion des instances et avait besoin d'une composante permettant d'établir le calendrier des instances, des salles d'audience et des juges selon les règles relatives à la gestion des instances et la circuiterie. La tentative visant à passer d'un système fondé sur un RLE (réseau local d'entreprise) à un système fondé sur un réseau longue portée s'est soldée par un échec, de sorte que les tribunaux se sont retrouvés sans la capacité de mettre en mémoire et de récupérer des données électroniques.

« L'initiative a aussi échoué parce que l'analyse de rentabilisation sous-jacente, qui était fondée sur la réduction immédiate des effectifs, comportait des lacunes », selon le juge Granger. « À court terme, l'introduction d'un système électronique ne réduira probablement pas le coût du personnel judiciaire ».

Le juge Granger a déclaré qu'il incombait à la magistrature de déterminer de façon indépendante les besoins présents et futurs des tribunaux en matière électronique.

« À moins que nous suivions cette politique, nous porterons atteinte à l'indépendance de la magistrature en impartissant à autrui la manière dont nous assumerons nos responsabilités ».

Les deux juges ont proposé une meilleure communication entre les groupes judiciaires traitant de la technologie au sein des tribunaux.

SURVEILLANCE INFORMATIQUE

Selon le Conseil, « [...] il est primordial de bien définir et d'être en mesure de justifier le but de la surveillance informatique des juges [...] La surveillance informatique doit respecter le caractère secret des délibérations, la confidentialité, le droit à la protection de la vie privée et l'indépendance de la magistrature ».

Le Conseil canadien de la magistrature a approuvé des lignes de conduite sur la surveillance des systèmes informatiques des tribunaux visant à protéger ces derniers des menaces à la sécurité sans compromettre la vie privée et l'indépendance de la magistrature.

Les lignes de conduite, élaborées par le Sous-comité sur la sécurité informatique du Comité consultatif sur l'utilisation des nouvelles technologies par les juges, ont été approuvées au cours de l'assemblée annuelle du Conseil tenue à Calgary à la fin de septembre et ont depuis lors été envoyées à tous les sous-ministres de la Justice.

Les lignes de conduite ont pour effet de reconnaître qu'une protection efficace des réseaux informatiques à l'encontre des menaces à la sécurité passe par des activités de surveillance. Toutefois, il est primordial de bien définir et d'être en mesure de justifier le but de cette surveillance, laquelle doit « respecter le caractère secret des délibérations, la confidentialité, le droit à la protection de la vie privée et l'indépendance de la magistrature », selon les lignes de conduite.

L'avis découle d'un séminaire que le Conseil a tenu en mars dernier sous la direction du Comité ainsi que des travaux du professeur Michael Geist, de la Faculté de droit de l'Université d'Ottawa, dont le

texte intitulé *Surveillance des ordinateurs et du courrier électronique en milieu de travail au Canada : de l'attente raisonnable en matière de respect de la vie privée à la surveillance raisonnable* est affiché sur le site Web du Conseil à l'adresse suivante : www.cjc-ccm.gc.ca.

Lignes de conduite sur la surveillance informatique

1. La surveillance informatique est, en général, exercée par l'intermédiaire d'un logiciel qui effectue un suivi des activités sur un ordinateur. Il est possible, entre autres, de faire le suivi des activités en réseau, des menaces à la sécurité, de l'utilisation de l'Internet, de la saisie de données, de l'échange de courriels et des autres façons dont les ordinateurs sont utilisés. La surveillance est effectuée par une autre personne que l'utilisateur, soit à sa connaissance, soit à son insu. Dans un cas comme dans l'autre, l'utilisateur n'a aucun droit de regard sur la surveillance ou les données recueillies.

2. Pour protéger efficacement les réseaux informatiques des menaces à la sécurité, une certaine surveillance est nécessaire. Dans certains cas, toutefois, la surveillance informatique peut menacer sérieusement l'indépendance de la magistrature et constituer par surcroît une atteinte illégale à la vie privée. Les présentes lignes de conduite visent à aider les juges et les administrateurs de systèmes à élaborer des pratiques de surveillance informatique adéquates.

3. Il est primordial de bien définir et d'être en mesure de justifier le but de la surveillance informatique des juges et du personnel judiciaire qui relève directement des juges. La surveillance informatique doit respecter le caractère secret des délibérations, la confidentialité, le droit à la protection de la vie privée et l'indépendance de la magistrature.

4. Les informations que les juges et le personnel judiciaire conservent sur leur ordinateur ne peuvent dans aucune circonstance faire l'objet de surveillance informatique. Il est par conséquent défendu, entre autres, de surveiller tout ce qui est tapé à l'ordinateur, l'échange de courriels, les documents créés à l'aide de texteurs ou les autres fichiers informatiques, la recherche juridique, les sites Internet visités et les fichiers téléchargés par chaque utilisateur.

5. Des mesures peuvent être prises pour surveiller le trafic du réseau, tenir un journal des erreurs et des exceptions et effectuer une maintenance conforme aux normes de l'industrie pour préserver l'intégrité des ressources partagées en réseau et protéger les systèmes informatiques contre les cyberpirates et les menaces à la sécurité.

6. La surveillance de la sécurité et de l'intégrité d'un système informatique :
   - n'est effectuée que pour des motifs légitimes, telles la vérification du rendement du réseau ou la gestion de la sécurité du réseau;
   - adopte l'approche la moins importune raisonnablement applicable dans les circonstances. Par exemple, si une activité en particulier a une incidence sur les ressources du réseau, les administrateurs du système devraient tenter d'obtenir la collaboration des juges et du personnel judiciaire leur faisant part de leurs préoccupations particulières en ce qui concerne les technologies de l'information;
   - ne recueille que des données d'ensemble. La surveillance des activités informatiques et des habitudes individuelles des juges ou du personnel judiciaire est prohibée, sauf s'il s'agit de vérifier si l'utilisateur a un droit d'accès valide.

7. Les données relatives à la surveillance doivent être gardées confidentielles. Seul le personnel des technologies de l'information responsable de l'intégrité et de la sécurité du système informatique qui a besoin de ces données y a accès. Les journaux tenus sur la surveillance électronique et les autres fichiers doivent être régulièrement purgés. Il est permis de conserver des statistiques de surveillance mais seulement à partir de données d'ensemble et en se limitant aux éléments qui concernent l'intégrité et la sécurité du système.

8. L'implantation de la surveillance informatique n'est jamais faite sans le consentement du juge en chef de la Cour. Les juges et le personnel judiciaire doivent participer activement à l'élaboration et à l'administration des pratiques en matière de surveillance informatique qui sont conformes aux présentes lignes de conduite. La surveillance informatique devrait être administrée par le personnel qui se rapporte directement au ou à la juge en chef de la Cour et qui relève directement de son autorité.

9. Les juges et le personnel judiciaire doivent être tenus au courant des avis par des notifications claires, évidentes et régulières qui les informent sur les pratiques de surveillance. Les cours devraient élaborer des lignes de conduite acceptables sur l'utilisation des ordinateurs et les communiquer aux intéressés lorsqu'on leur accorde un accès aux ordinateurs pour la première fois. Dès la mise en marche de l'ordinateur, l'écran devrait régulièrement afficher un rappel de l'existence et la raison des lignes de conduite sur la surveillance électronique et des raisons qui la justifient.

SÉCURITÉ Q & R

par Lewis Eisen & Martin Felsky

Q. : J'ai entendu dire que, lorsqu'on supprime un document, ce document n'est pas réellement éliminé. Qu'en est-il?

R. : C'est vrai. Bien que vous ne voyiez pas les dossiers que vous avez supprimés, ils demeurent bel et bien présents dans votre appareil.

Lorsque vous supprimez un dossier au moyen d'une méthode courante (comme de faire glisser ce dossier jusque dans la corbeille), l'espace disque où le dossier est stationné affiche « vacant ». Le dossier lui-même n'est pas déplacé. Les logiciels courants réagissent à l'enseigne « vacant » en omettant d'afficher le dossier en question dans leurs listes de dossiers du disque, de sorte que ce dossier cesse effectivement d'être visible.

L'ordinateur ne prend pas la peine d'éliminer les données puisque, éventuellement, celles-ci seront écrasées par le dossier suivant que le système garera dans l'espace occupé par ces données. Jusqu'à ce que le dossier soit écrasé, toutefois, il est repérable au moyen d'un fureteur de dossiers, un type de logiciel qui ne tient pas compte des enseignes « vacant » et qui scrute chaque espace du disque pour vérifier ce qui s'y trouve.

Cette pseudo-suppression est censée être une caractéristique de l'ordinateur et non un bogue. Elle permet non seulement d'accélérer le processus d'élimination, comme vous le constateriez si vous tentiez d'éliminer des centaines de dossiers à la fois, mais également de reconstituer un document supprimé par erreur. Cependant, elle comporte également un risque lié à la sécurité; en effet, même un document qui est censé avoir été détruit n'est pas à l'abri des yeux indiscrets.

Est-ce que cette persistance des données devrait vous préoccuper? Dans des circonstances normales : non. Si vous êtes maître de l'accès à votre disque, vous pouvez y laisser vos dossiers supprimés, qui seront éliminés au fur et à mesure de la réutilisation de l'espace qu'ils occupent.

Il en va autrement si vous prévoyez vendre votre ordinateur ou vous en départir d'une façon ou d'une autre. Dans un tel cas, vous ne pourrez vous permettre de laisser la moindre trace de données. Avant de remettre votre ordinateur, vous devriez pratiquer un nettoyage systématique de votre disque. À cette fin, vous aurez besoin d'un utilitaire spécifique. Le logiciel Norton Utilities, par exemple, est muni d'une application « *wipe* » (« nettoyer »), qui élimine les dossiers supprimés et les vestiges de dossiers.

Le processus d'élimination décrit au premier paragraphe s'applique aux documents et aux fichiers de programmes que vous effacez à l'aide des commandes de suppression fournies par le *système d'exploitation* (MS Windows ou Macintosh). Il ne s'applique pas nécessairement au courriel ou aux autres textes supprimés à l'aide des commandes existant à l'intérieur d'un logiciel.

La façon dont les données sont supprimées et dont l'espace du disque est récupéré varie d'un programme à l'autre. Si vous ne vérifiez pas la documentation technique qui accompagne chaque programme, vous ne saurez pas jusqu'à quel point les données que vous supprimez peuvent être récupérées; de plus, même si vous prenez connaissance de cette documentation, il se peut qu'elle ne soit pas suffisamment claire ou précise.

Afin d'obtenir une sécurité maximale, ne vous fiez pas aux commandes de suppression du système d'exploitation ou de vos logiciels. Avec un utilitaire de nettoyage du disque, vous ne faites pas que cacher vos données : vous les effacez en permanence. Alors seulement serez-vous assuré(e) que vos documents n'ont pas subsisté et ne risquent pas d'être débusqués par quelqu'un qui s'intéresse à vos données.

Lewis S. Eisen, B.A., J.D., agent de formation principal — JUDICOM, Bureau du Commissaire à la magistrature fédérale.

Martin Felsky, Ph.D., président et avocat général de Commonwealth Legal (Toronto).